

**FINAL**

**OSD / JOINT STAFF**

**INTEGRATED  
VULNERABILITY  
ASSESSMENT (IVA)**

**INTEGRATED PROCESS  
TEAM (IPT)**

**FINAL REPORT**



**Office of the Assistant Secretary of Defense  
Command, Control, Communications,  
and Intelligence (C3I)**



**Joint Staff  
Director for Strategic Plans & Policy (J-5)  
Deputy Director for Pol-Mil Affairs/ Global**

---

**FINAL**



OFFICE OF THE SECRETARY OF DEFENSE

1000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1000



July 31, 2001

This report addresses two important issues that confront the Department of Defense in developing a fully informed capability to respond to the challenges and demands of executing the National Military Strategy: critical infrastructure protection and the assessment of infrastructure vulnerabilities.

Our military strength is based on information superiority that permits the application of worldwide power projection and overwhelming full spectrum dominance. Because of this, our physical and information infrastructures increasingly become high value targets in the sights of any adversary. In order to achieve mission assurance we must have a full appreciation for the inventory of our critical infrastructures, as well as an understanding of their vulnerabilities so that our combatant commanders can practice the most informed risk management.

The Integrated Vulnerability Assessment Integrated Process Team brought together a diverse group of infrastructure owners and assessment experts, in an effort to determine the best methods for providing this important vulnerability assessment support to the combatant commanders.

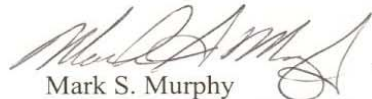
It has been a pleasurable and rewarding challenge for us to serve as the co-chairs of this Team. We believe that we have assembled findings and recommendations that will support a rational, improved method for assessing infrastructure vulnerabilities and sharing the collected information with the full range of asset owners and users. This report, though, should only be seen as the beginning. Ultimate success will require decisive implementation of the recommendations, with associated hard work over time by the appropriate subject matter experts.

The input of every participant in this project was crucial to the finished product. The collection of assessment data and presentation of the Findings, in particular, represent the collective efforts of all concerned. The co-chairs made the ultimate determination on the wording and presentation of the recommendations. We cannot take credit for the quality of the ideas presented, as they are based on the input of many, but we must solely accept blame for any shortfalls or confusions that resulted from our approach.

  
Josephine M. MacMichael

Financial Manager

Critical Infrastructure Protection Directorate

  
Mark S. Murphy

Lieutenant Colonel USMC

J-5 Homeland Security Division

FEDERAL RECYCLING PROGRAM



PRINTED ON RECYCLED PAPER

---

FINAL

## TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY</b>	<b>ES-1</b>
<b>1.0 INTRODUCTION</b>	<b>1</b>
1.1 PURPOSE	1
1.2 SCOPE	1
1.3 BACKGROUND	1
1.4 CHARTER AND TERMS OF REFERENCE (TOR)	3
1.5 DEFINITIONS	4
1.6 APPROACH	5
<b>2.0 FINDINGS</b>	<b>7</b>
2.1 QUESTION 1:	7
2.2 QUESTION 2:	10
2.3 QUESTION 3:	13
<b>3.0 RECOMMENDATIONS</b>	<b>16</b>
3.1 VISION	16
3.2 RECOMMENDATIONS	16
<b>APPENDIX A – CHARTER AND TERMS OF REFERENCE</b>	<b>A-1</b>
<b>APPENDIX B – LIST OF REPRESENTATIVES</b>	<b>B-1</b>
<b>APPENDIX C – RELATIONSHIP OF TASKS TO QUESTIONS</b>	<b>C-1</b>
<b>APPENDIX D – ASSESSMENT MATRIX</b>	<b>D-1</b>
<b>APPENDIX E – RECOMMENDATIONS MATRIX</b>	<b>E-1</b>
<b>APPENDIX F – BRIEFINGS</b>	<b>F-1</b>
APPENDIX F1 – DOD INTEGRATED VULNERABILITY ASSESSMENT (DIVA)	F1-1
APPENDIX F2 – ROCKY MOUNTAIN EFFORT	F2-1
APPENDIX F3 – CRITICAL INFRASTRUCTURE PROTECTION (CIP) ANALYSIS & ASSESSMENT CRITICALITY	F3-1
APPENDIX F4 – MISSION DEGRADATION ANALYSIS PROJECT OVERVIEW	F4-1
APPENDIX F5 – NATIONAL SECURITY AGENCY INFORMATION ASSURANCE ASSESSMENTS	F5-1
APPENDIX F6 – AT/FP PROGRAM OVERVIEW	F6-1
APPENDIX F7 – BALANCED SURVIVABILITY ASSESSMENTS	F7-1

<b>APPENDIX F8 – DEFENSE SECURITY SERVICE INDUSTRIAL SECURITY PROGRAM (FACILITY SECURITY CLEARANCE AND SECURITY REVIEW PROCESSES)</b>	<b>F8-1</b>
<b>APPENDIX F9 – DISA'S SECURITY READINESS REVIEW (SRR) PROCESS</b>	<b>F9-1</b>
<b>APPENDIX F10 – JPO-STC INFRASTRUCTURE ASSURANCE PROGRAM OVERVIEW FOR THE IVA-IPT</b>	<b>F10-1</b>
<b>APPENDIX F11 – AIR FORCE VULNERABILITY ASSESSMENTS</b>	<b>F11-1</b>
<b>APPENDIX F12 – INFORMATION BRIEFING FOR: INTEGRATED VULNERABILITY ASSESSMENT INTEGRATED PROCESS TEAM (USTRANSCOM)</b>	<b>F12-1</b>
<b>APPENDIX F13 – SECURITY, FORCE PROTECTION, AND LAW ENFORCEMENT DIVISION, ODCSOPS</b>	<b>F13-1</b>
<b>APPENDIX F14 – THE DLA COMBATING TERRORISM PROGRAM</b>	<b>F14-1</b>
<b>APPENDIX F15 – NAVAL INTEGRATED VULNERABILITY ASSESSMENT (NIVA)</b>	<b>F15-1</b>
<b>APPENDIX F16 – CHIEF OF NAVAL OPERATIONS INTEGRATED VULNERABILITY ASSESSMENT (CNOIVA) PROGRAM</b>	<b>F16-1</b>
<b>APPENDIX F17 – ARMY INFRASTRUCTURE ASSURANCE XXI</b>	<b>F17-1</b>
<b>APPENDIX F18 – MARINE CORPS INTEGRATED VULNERABILITY ASSESSMENT (MCIVA)</b>	<b>F18-1</b>
<b>APPENDIX F19 – COMBATANT COMMAND SUPPORT DESIRES CIP VULNERABILITY ASSESSMENT</b>	<b>F19-1</b>
<b>APPENDIX F20 – IVA NOTIONAL TIMELINE MATRIX (SPREADSHEET)</b>	<b>F20-1</b>
<b>APPENDIX F21 – PACNORWEST CIP ANALYSIS AND ASSESSMENT PROCESS LESSONS LEARNED</b>	<b>F21-1</b>
<b>APPENDIX F22 – MALMSTROM AFB ASSESSMENT</b>	<b>F22-1</b>
<b>APPENDIX F23 – ROCKY MOUNTAIN EFFORT (RMC) LESSONS LEARNED</b>	<b>F23-1</b>
<b>APPENDIX F24 – JSIVA SCHEDULING PROCESS (JOINT STAFF INTEGRATED VULNERABILITY ASSESSMENT)</b>	<b>F24-1</b>

## EXECUTIVE SUMMARY

During January – May 2001, the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD (C3I)) and the Joint Staff (J-5, Global) sponsored an Integrated Vulnerability Assessment (IVA) Integrated Process Team (IPT). The purpose of this IPT was to study the viability of a critical infrastructure protection (CIP) focused vulnerability assessment process. As such, the IPT was chartered to undertake the seven tasks listed in Appendix A. In general, these tasks were to review current assessment initiatives with respect to funding, oversight control, scheduling, information requirements, and information sharing and to make recommendations on the implementation of an IVA process.

Between 1 February 01 and 8 March 01, we received a series of briefings from Department of Defense (DoD) organizations performing vulnerability assessments and inspections related to force protection/antiterrorism, information assurance, cleared contractors, and the security of other infrastructures. Briefings were also provided on CIP analysis efforts, lessons learned from OASD (C3I) CIP Directorate sponsored assessment demonstration projects, and feedback from CINC outreach efforts. The background provided by these briefings led us to conclude that we could not adequately address the seven tasks in our charter within the time allotted. Consequently, with the concurrence of our Steering Committee, we formulated and addressed the following three questions that cover certain areas of these tasks. The relationship of the three questions to the original seven tasks is shown in Appendix C.

- Question 1: Are we satisfying CIP requirements for determining if critical assets are vulnerable?
- Question 2: Are we collecting information effectively and efficiently?
- Question 3: Are the people who need the assessment results getting the information they need?

We addressed Question 1 through the macro level, core competency assessment matrix found in Appendix D and through a set of “working” CIP requirements that served as a proxy for formally established DoD requirements. Questions 2 and 3 were addressed through discussions of comparative practices of the Services, Agencies and assessing organizations. Through a series of discussions and working meetings, we arrived at a consensus of findings regarding the state of vulnerability assessments within DoD, especially as they are applicable to critical infrastructure.

Based on these findings, the IVA IPT co-chairs prepared a set of draft recommendations. These were shared throughout the IPT for review. Comments and other inputs have either been incorporated into the final recommendations presented below, or have been otherwise addressed. While generally supported by the IPT membership, these recommendations do not represent the same level of consensus as found in the findings.

In general, our review found that there is a wide range of assessments being performed throughout the Department. Many of these assess infrastructure vulnerabilities either directly or indirectly. Highly qualified and well-led assessment specialists operate under the cognizance of various agencies and programs. The Services, in particular, have very broad and robust assessment/inspection programs that derive directly from their Title 10 responsibilities to organize and maintain forces available for execution of missions in support of combatant commander mission requirements. However, lacking a solid departmental policy on what infrastructure is critical (what to assess) as well as on standards for frequency of assessment (when to assess) and standards of vulnerability (how to assess), it is not possible to determine fully the gaps and overlaps that exist among current assessments.

Operating in a system of decentralized execution, the various assessments produce numerous reports on vulnerabilities throughout the department. However, no common standard exists for report format or distribution, resulting in cubby-holed information of great specificity, routinely available only to local commanders. These local commanders have primary responsibility for risk management decisions in support of their designated missions. However, they do not always have the necessary perspective to make their decisions within the context of the broader impacts that their local missions have on broad areas impacting combatant commanders. In addition, resource channels within the Services and Agencies do not always have ready access to the information that would support particular fixes. Finally, the various assessment organizations lack a ready access to the information generated among them, both in terms of raw data and trend analysis. This results in an experience of assessment repetition at the local level as well as a reduced ability for assessment organizations to leverage existing products in support of in-depth and continuing vulnerability analysis.

Ultimately we concluded that the essentially decentralized nature of vulnerability assessments in the department is a positive characteristic that should be maintained. The necessity for a centrally mandated Defense Integrated Vulnerability Assessment to support CIP assessment requirements was not validated. However, our report does recommend a number of procedural and structural adjustments that would increase efficiency without degrading efficacy. Policy fixes, assessment coordination, and report sharing are highlighted. Finally, designation of an executive agent for assessments could lead to improved standardization and efficiency. These recommendations are matched to tasks, with proposed implementation agencies, in Appendix E.

# **1.0 INTRODUCTION**

## **1.1 PURPOSE**

The purpose of the Integrated Vulnerability Assessment (IVA) Integrated Process Team (IPT) was to develop the end-state and associated milestones to implement a critical infrastructure protection (CIP) integrated assessment process. The IPT was to address the current assessment initiatives with respect to funding, oversight control, scheduling, information requirements, and information sharing. The IPT was to further investigate the applicability and feasibility of an integrated assessment process.

## **1.2 SCOPE**

The IPT was chartered to study the viability of an integrated vulnerability assessment process to support assessments of critical infrastructure protection vulnerabilities. The IPT was directed to make recommendations, as appropriate, on the implementation of an IVA process, maximizing to the largest extent possible the processes and protocols of existing assessments.

## **1.3 BACKGROUND**

The Defense Critical Infrastructure Protection (CIP) Program addresses the question of how the loss or degradation of a critical capability/asset affects our warfighting ability, and ultimately our national defense and economic security. The program approach is enterprise-oriented in scope. PDD-63 requires every department and agency of the Federal Government to protect its critical infrastructure and to establish procedures for the conduct of vulnerability assessments. The Department of Defense Critical Infrastructure Protection Plan dated 18 November 1998 provides for an infrastructure analysis and assessment process that includes vulnerability assessments at the Defense-wide, Sector, installation, and asset levels of the infrastructure. The CIP analysis and assessment process provides the basic framework to support the identification and prioritization of remediation and mitigation efforts as well as the execution of consequence management activities. Based on CINC identified critical requirements, the analytical process provides for the examination of the dependencies and inter-dependencies, from warfighter to supporting DoD and commercial and industrial infrastructures, to determine what assets are critical. The assessment process allows for validation of criticality, development of identified dependencies and assets for analysis, identification of critical asset vulnerabilities, and suggestion of countermeasures.

A number of excellent vulnerability assessment efforts exist that, while chartered to satisfy other valid objectives, can also provide insight into aspects of infrastructure vulnerabilities. The Joint Staff Integrated Vulnerability Assessment (JSIVA) and the Balanced Survivability Assessment (BSA), both conducted by the Defense Threat Reduction Agency (DTRA), the Infrastructure Assurance Program (IAP) Assessment conducted by the Joint Program Office-Special Technology Countermeasures (JPO-STC), and the Information System

Security (INFOSEC) Assessment conducted by the National Security Agency (NSA) are but four of these. The JSIVA was established as an anti-terrorism/force protection assessment, designed specifically to respond to the requirements of DoD Directive 2000.16. As such, it examines an installation's vulnerability to a mass casualty terrorist attack and provides procedural and technical options for reducing the risk to installation personnel. JSIVAs are targeted at all DoD installations with 300 or more personnel. While JSIVAs focus on personnel protection, BSAs are mission-oriented assessments of critical systems and their supporting infrastructures. BSAs have typically been conducted at nuclear command and control facilities. JSIVAs and BSAs are primarily inward looking, while IAP assessments focus primarily on external commercial infrastructures (i.e., energy, telecommunications, transportation, and water) that support installations. The purpose of an IAP assessment is to characterize these infrastructures and to assess the effects of critical link or node disruptions to the installation as they impact a specific mission. INFOSEC Assessments conducted by NSA have a cyber focus in contrast to the more broadly based assessments described above. INFOSEC Assessments provide a review of an organization's information systems security posture and make specific recommendations about how to improve it. These assessments are conducted for DoD installations/facilities, DoD contractors, civil agencies, and others deemed critical to the national security information infrastructure.

The four assessments highlighted above are only examples. The Services and Agencies conduct their own assessments and inspections as well. Numerous assessments are currently being conducted for purposes other than CIP. These assessments vary in scope, depth, and frequency, and may or may not be coordinated. As a result, and as discussed at the Fall 2000 CINC's Conference, the number of independent, but somewhat overlapping assessments is perceived to have a negative impact on already busy installation personnel.

Over the last two years, the OASD (C3I) CIP Directorate has conducted several demonstration projects to examine the feasibility of leveraging existing assessment methodologies to support a CIP analysis and assessment process, with an eye towards applying lessons learned to a potential Defense-wide integrated vulnerability assessment. The first such project took place in July 1999 in Norfolk, Virginia. Dubbed the Tidewater Exercise, its purpose was to form a collaborative partnership between a major commercial infrastructure provider, the Navy, JPO-STC and other DoD participants in order to identify and potentially remediate critical asset and infrastructure vulnerabilities. The Tidewater Exercise successfully demonstrated the importance of information sharing between DoD and commercial infrastructure providers. It also demonstrated that a previously unidentified single failure point, having regional consequences, might become apparent through application of a disciplined infrastructure analysis and assessment process. Accordingly, the PACNORWEST demonstration project that followed between January-September 2000 was conducted around Puget Sound guided by a regional focus. The greater scope and complexity of this project demonstrated the need for solid preparation and agreement between organizations in advance of actual analysis and assessment execution. Necessary coordination includes establishing roles and responsibilities among participants, setting realistic goals and expectations, providing for information sharing among assessment organizations, and establishing a mission focus. PACNORWEST was a coordinated rather than an integrated assessment.

---

**FINAL**



The third demonstration project, Malmstrom Air Force Base, was conducted over a two-week period in July-August 2000 and provided the first attempt at an integrated assessment involving JSIVA, BSA and JPO-STC teams. This effort focused on a single installation with a single dominant mission. At Malmstrom, assessment teams collected information simultaneously and participated in some limited joint analysis; however, the different foci of the individual assessments precluded producing a truly integrated assessment. Malmstrom provided an opportunity to observe the similarities and differences among teams and assessment protocols, to further understand the potential problems in information sharing and reuse, and identified the importance of establishing a single point of contact with the installation for assessment coordination.

A fourth demonstration project, the Rocky Mountain Corridor (RMC) assessment, is ongoing. RMC has built on the lessons learned from the previous projects and consequently has changed in scope and orientation since its start in late 2000. Originally conceived as a regional assessment following the PACNORWEST model, RMC has become mission-oriented and includes installations/facilities in Canada and the United States that support the U.S. Space Command's Integrated Tactical Warning and Attack Assessment (ITW/AA) mission. RMC is neither comprehensive in scope (due to resource limitations) nor has it succeeded in removing all obstacles to effective information sharing. However, it will result in an integrated report for use by the CINC in assessing the potential impact of critical infrastructure vulnerabilities upon the ITW/AA mission.

These prototype projects identified the wide-ranging challenges to implementing an approach that would be supportive of CIP efforts. Accordingly, OASD(C3I) with the concurrence of the Director of the Joint Staff established the IVA IPT to look into the possibility of better synchronizing assessments and fostering synergy through the assessment process.

#### **1.4 CHARTER AND TERMS OF REFERENCE (TOR)**

The Charter and Terms of Reference for the IVA IPT are attached at Appendix A. The Deputy Assistant Secretary of Defense for Security and Information Operations signed the charter establishing the IPT on January 16, 2001. The Charter set objectives, defined responsibilities, delineated seven tasks for the IPT, and asked for a final report four months after the start of the IPT. The TOR provided the operating principles for the conduct of the IPT.

The Charter identified OASD (C3I)/CIP Directorate and the Joint Staff (J-5 Global) as the sponsors of the IPT and tasked them to provide guidance and joint direction to the effort. The sponsors were tasked with appointing representatives to co-chair the IPT. The Charter directed that the membership consist of representatives from the following organizations: Office of the Secretary of Defense (Command, Control, Communications and Intelligence and Special Operations/Low Intensity Conflict), Joint Staff (J-2, J-34, J-4, J-6 and J-7), the Services, U.S. Transportation Command (USTRANSCOM), Defense Threat Reduction Agency (DTRA), Defense Information Services Agency (DISA), Defense Logistics Agency (DLA), Defense

Security Services (DSS), National Security Agency (NSA), and Joint Program Office – Special Technology Countermeasures (JPO-STC). A listing of the primary and alternate representatives to the IPT is provided at Appendix B.

The Charter laid out the following seven tasks for the IPT to consider:

- Study the current assessment processes to determine the authority/policy source for individual assessment mandates, the applicable standards and documentary authority for the associated assessment standards, how individual assessments are scheduled, the required frequency of assessments, specific data collection requirements, and the required reports/distribution of reports.
- Study the CIP specific assessment requirements. Answer the questions – “What do we want to assess?” “Why do we need/want to assess?”, “What will we do with the information when we have gathered it?”, “Who needs to know?”, “What form do the results need to be promulgated in?” “What additional security requirements have we created in an IVA process?”
- Explore methods to synergize current individual assessments that might directly support CIP. Assessment integration would focus on reduction of any redundancies, development of clear assessment standards, development of common protocols for assessment, streamline scheduling, and economize funding. Any effort to combine assessments must be consistent with existing policy directives or recommend appropriate changes to policy directives for assessments.
- Make recommendations on how the results of CIP assessments should be used in planning, mitigation, and remediation. Determine how to best use the collected data to ensure that appropriate CIP remediation/mitigation measures are implemented.
- Develop a process, with timelines, for the planning, coordination, and scheduling of IVA assessments. Address timelines for generation, coordination and review of IVA reports.
- Determine how, to whom, and in what format the IVA results should be distributed.
- Conduct a review of organizational roles and responsibilities to determine the most appropriate organizational location for the oversight, ownership, and management of an IVA Teams and process.

## **1.5 DEFINITIONS**

For the purposes of this report, we used the following definitions:

Asset, Infrastructure, or Resource Owner - Within DoD, the organizational element that controls, directs and has custody of the critical asset or resource. For non-DoD assets,

e.g., commercial and industrial assets or infrastructure, the DoD organizational element that controls, directs, and has responsibility for the contract or agreement through which the critical service or product is provided.

**Critical asset** – Any asset that is designated as essential to a vital DoD mission, interest or capability.

**Defense Critical Infrastructure** – Those systems and assets essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy.

**Critical Infrastructure Protection** – CIP is the identification, assessment, and assurance of Cyber and Physical infrastructures that support mission critical capabilities and requirements, to include the political, economic, technological, and informational security environments essential to the execution of the National Military Strategy.

**Protocol** - The defining structure, framework, and methodology of a particular assessment which differentiates it from some other assessment. Elements include charter legislation or regulation, scheduling mechanisms, designated team structure, formal standards, checklists or other prescribed assessment tools, reporting formats and distribution, and lessons-learned generation and distribution. In its most refined form, an established protocol would permit replication of a given assessment by various assessment agencies.

**Vulnerability** – A characteristic of a critical infrastructure’s design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

## **1.6 APPROACH**

The Steering Committee members, Mrs. Bonnie Hammersley, representing OASD (C3I), and Colonel Joseph Dunford, USMC, representing J-5, appointed Mrs. Jo MacMichael and LtCol Mark Murphy, USMC, to represent their respective organizations as co-chairs of the IPT.

In accordance with the TOR, the focus of the kick-off meeting was to review the IVA IPT charter with the team and to elicit their comments and feedback. The co-chairs’ review of the charter was followed by a detailed discussion of the seven tasks, the objectives, deliverables and reports to be provided to the Steering Committee.

The IPT membership represented two groups: those who work CIP and those who conduct assessments. Therefore, our next objective was to quickly establish a common level of knowledge on both subjects. Team members arranged for presentations on vulnerability assessments performed by their organizations. These included assessments relating to force protection/antiterrorism, information assurance, cleared contractors, and assurance of other

infrastructures. The Air Force also provided substantial information on command inspections. In addition, briefings were provided on CIP analysis efforts, lessons learned from the CIP Directorate-sponsored assessment demonstration projects discussed above, and feedback from the CINC outreach efforts.

Based on the briefings received and subsequent discussions, the Co-chairs and the team concluded that the IPT should not attempt to address all of the assigned tasks, because of time limitations. Instead, the group developed a set of three questions through which it would address composite issues. With the subsequent concurrence of the Steering Committee, the IPT then directed its work to address each of these questions:

- Are we satisfying CIP requirements for determining if critical assets are vulnerable?
- Are we collecting information effectively and efficiently?
- Are the people who need the assessment results getting the information they need?

The relationship among the seven tasks and the three questions is delineated in Appendix C. Some elements of those tasks were excluded from IPT consideration. The findings from the deliberations of the IPT on these three questions are presented in Section 2.0. These findings capture a full consensus of all participants generated in more than twelve hours of dedicated discussion.

The next step in the process was to formulate recommendations to deal with the findings of the IPT. The recommendations are presented in Section 3.0. The recommendations were drafted by the co-chairs and presented to the members for review and comment. In many cases comments and other input were adopted directly into the recommendations. It would not be accurate, though, to characterize the recommendations as representing the same level of consensus as that found in the Findings.

## 2.0 FINDINGS

### 2.1 QUESTION 1:

#### **ARE WE SATISFYING CIP REQUIREMENTS FOR DETERMINING IF CRITICAL ASSETS ARE VULNERABLE?**

**Finding 1:** Coverage. Gaps and overlaps in assessment areas exist within DoD. Our methodology does not provide the granularity to identify specific gaps and overlaps.

**Finding 2:** Capability. The range of assessments currently performed indicates the skill mix to conduct CIP assessments is resident among the various assessment agencies.

**Finding 3:** The adequacy of resources to address CIP assessment requirements currently cannot be determined.

#### **Discussion:**

To address Question 1, it is necessary to understand both the characteristics and applicability of current assessment processes (Task 1) and to understand what constitutes CIP requirements (Task 2). In order to gain an understanding of current assessment processes, Service and Agency representatives with assessment responsibilities were asked to brief us on the following topics:

- Assessment authority and objectives
- Funding
- Team size and composition
- Assessment protocols and standards
- Intended audience
- Assessment products and reports
- Infrastructure addressed

We received 20 assessment and inspection related briefings over the 1 February 01 – 8 March 01 period. Additional briefings were presented on special topics such as lessons learned from OASD C3I-sponsored demonstration projects and on Service CIP assessment initiatives.

These briefings are included as appendices to this report. We condensed this information into the assessment matrix found at Appendix D and subsequently used it in addressing Question 1.

As part of the Defense Threat Reduction Agency's Mission Degradation Analysis (MIDAS) program, Science Applications International Corporation (SAIC) analysts developed a more detailed assessment matrix as part of the MIDAS requirement definition. MIDAS is a research and development effort to develop automated tools to assess the degradation of critical infrastructures and the impact of these degradations on DoD missions. The MIDAS assessment matrix could be a good starting point for any working group charged with examining the details of gaps and overlaps among the various assessments.

Assessors were asked to arrange for briefings on their organization's inspections or assessments that were applicable to some aspect of determining critical asset vulnerability. We could not determine at this point whether or not these assessments, either as a group or individually, satisfy CIP assessment requirements. There are at least two reasons for this. The first is the absence of a DoD policy that specifically identifies the scope, applicability, standards, or information sharing and reporting procedures to meet CIP assessment requirements. The second reason is simply a matter of resources. A focused and disciplined consideration of this topic would require more time than was available to us.

As noted in Section 1.3, PDD – 63 requires every department and agency of the Federal Government to protect its critical infrastructure and to establish procedures for the conduct of vulnerability assessments. DoD's approach to meeting this requirement was to use capabilities found in its Critical Asset Assurance Program (CAAP), as described in DoD Directive (DoDD) 5160.54. This directive states that, "It is DoD policy to provide an integrated asset and infrastructure vulnerability assessment and assurance program for the protection and assurance of DoD and non-DoD Critical Assets worldwide through CAAP." The CAAP, however, did not receive the funding necessary to establish the capabilities described in DoDD 5160.54. DoD is reviewing a new CIP directive that will replace DoD Directive 5160.54. In its current draft, this replacement directive does not directly address the need to establish a CIP assessment capability. The continued absence of formally established DoD CIP assessment requirements is a major impediment to our work.

Lacking such a set of requirements or protocols, we used the following "working CIP requirements" as a proxy to address Question 1:

- Employs a Defense-wide set of standard protocols to conduct a comprehensive mission-oriented, integrated critical asset and infrastructure vulnerability assessment
- Leverages "best practices" of established assessment and inspection processes including appropriate elements of force protection, anti-terrorism, physical security, operations security (OPSEC), business continuity, commercial infrastructure assurance, information security/assurance and personnel security, nuclear surety, and operational readiness

- Addresses CONUS and OCONUS, on-base and off-base (commercial, industrial, host nation) infrastructure, and other assets
- Ensures the ability for information sharing and reuse

Based on the above, we constructed a macro level, core competency assessment matrix as shown in Appendix D. Using this approach, we concluded that one or more current assessments occur in all criteria areas (i.e., cyber, physical, industrial-base, commercial, CONUS and OCONUS). However, we also determined that there are gaps and overlaps in the current assessment coverage of critical infrastructure (Finding 1). We found that among the areas not adequately covered are the industrial-base, and OCONUS/host nation infrastructures and other assets. We observed that some smaller Defense Agency activities do not receive consistent and detailed assessment assistance available to larger components of the Department. In addition, coordination and dependency analyses across DoD components to support assessments are lacking.

Besides the absence of adequate coverage in the industrial base, we further noted that the CIP assessment process does not consider all factors affecting commercial and industrial asset assurance; for example, the asset's fiscal and business survival, necessary surge capacities, and product and service quality. Those factors can just as certainly deny the combatant commander the use or adequacy of a critical asset as can the loss of cyber or physical infrastructure. In defining CIP analysis and assessment policies the Department must decide how to consider and incorporate these factors. Other agencies within DoD and elsewhere in the federal structure collect, maintain and evaluate some of that information. For example, likely sources would be the involved contracting or acquisition authorities and the USD(AT&L) Industrial Preparedness Program operating under DLA.

Critical assets and infrastructures vary widely in complexity, size, location, function, etc. Commercial and industrial base infrastructures and assets have further variances in their administrative, operational, and control environments. The CIP assessment process has to accommodate those variances to better conserve resources, minimize the assessment load on the asset, and ensure a timely assessment product.

Additional work would be needed to determine the entire spectrum of gaps and overlaps resulting from the scope and depth of the individual assessments. In addition, we believe that there are other assessments and other processes (e.g., exercise and war game experiences and lessons-learned) that have CIP-applicability that we did not include.

In reviewing the core competencies as identified in the assessment matrix, we found that the skill mix to conduct CIP assessments is resident among the various assessment agencies represented on the IPT (Finding 2). We believe this finding to be generally true; however, its proof will be in the application of assessments to the full range of Tier 1 and Tier 2 assets. As defined in the DoD CIP Execution Plan (CY00), Tier 1 assets are considered to be [DoD or non-

DoD] assets, the loss or degradation of which, would result in strategic mission failure for the warfighter. Tier 2 assets are defined as those assets, the loss or degradation of which, would result in Sector or element strategic functional failure, but strategic mission of the warfighter is still accomplished. The Joint Staff, CINCs, Services, Agencies, and Sectors are in the process of identifying these assets.

All of the above leads to the third finding that the adequacy of resources to address CIP assessment requirements currently cannot be determined. A determination of resource adequacy requires: 1) a set of formally adopted CIP assessment requirements, 2) an identified universe of critical assets (i.e., a tiered asset list), and 3) a resource baseline. None of these items currently exists.

The bottom line is that completely addressing Question 1 requires additional analysis.

## 2.2 QUESTION 2:

### **ARE WE COLLECTING INFORMATION EFFECTIVELY (SCHEDULING) AND EFFICIENTLY (TIMING)?**

**Finding 4:** Focus. The objective of the CIP program is CINC mission assurance through risk management of critical infrastructure vulnerabilities. This CINC mission assurance orientation is only partially addressed by the current assessment processes.

**Finding 5:** Scope. A geographically focused assessment (either regional or installation) may not fully address CINC operational mission assurance.

**Finding 6:** No DoD Critical Infrastructure (CI) tiered asset list exists. While this list is seen as the eventual foundation for prioritizing critical infrastructure for CINC mission assurance, there is no clearly defined interim process for CIP prioritization (and selection) of assets to be assessed.

**Finding 7:** There is currently no requirement to coordinate or integrate planning, execution, and reporting of the various assessments in support of DoD CIP objectives.

**Finding 8:** The DoD CIP Program lacks a formally coordinated policy directive that identifies assessment requirements, roles and responsibilities.

**Finding 9:** Sharing of information across assessment organizations in order to support coordinated and integrated efforts is hampered in part by the fact that some of the individual protocol standards are subjective vice objective.

**Finding 10:** No framework for integrating reports exists thus impacting (or diminishing) the ability to prioritize findings/results from a CIP perspective.



**Finding 11:** No formal, standardized mechanism exists for following up on findings across assessments.

**Discussion:**

Tasks 3, 5, and 7 address the need to review current assessment processes (and their associated roles and responsibilities) in order to directly support CIP. The goal was to reduce unwarranted redundancies if they exist, to develop common assessment standards and protocols, and to develop a process for better planning, coordination, scheduling, and review of assessments and assessment reports. Question 2 addresses two separate pieces of the information collection process: efficiency and effectiveness. These twin goals involve planning, scheduling, timing, and execution of assessments. They are inter-related and substantially influence the impact of assessments on installation resources.

Increasing efficiency through the synergy of multiple assessments is dependent on when a specific assessment is accomplished relative to other assessments. From the perspective of the current assessments, which are usually installation focused, this issue is largely irrelevant. But for CIP assessments, which should focus on an organization's ability to execute its assigned missions(s) and on accurately portraying interdependencies among infrastructures and critical assets, the issue is significant. If the assessments are accomplished at different times over an extended period, changes may have occurred making the resulting analysis of interdependencies inaccurate, adversely affecting the utility of the analysis, the value of the assessment, and the credibility of the process. For example, during the PACNORWEST vulnerability assessment, information from a previously conducted commercial assessment was included in the out-briefing to the installation commander. Although the briefing to the installation commander contained a caveat that the information was dated and might no longer be valid, the outdated information brought into question the usefulness of the assessment process.

The scheduling issue is related to the timing issue but is concerned with maximizing resources and minimizing the impact on installations being assessed. Discussions centered on the issue as to whether or not there are methods to achieve better synergy between current individual assessments that might directly support CIP while at the same time reducing the impact on the assessed organizations. The burden of assessments on installations was a recurring theme during our discussions based on anecdotal data. Despite the absence of hard factual evidence that installation resources are being overburdened, we believe that reducing the impact on installations should be an objective for our effort.

Even though we envision a planned sequential and predictable routine environment for the vulnerability assessment process, the supporting procedures and resources would ideally be able to execute unexpected and highly time sensitive assessments. We know, as shown in Desert Shield and Desert Storm, that assets not previously ranked as critical or not given a high priority for assessment, or assessed some time ago, suddenly increase in importance. Loss of production means, for example in a foreign country, of a single source for a key manufacturing part for a critical asset weapon system, will suddenly make an alternative source, when one is located, a critical asset. The current CIP related assessment processes and procedures do not account for

quick reaction assessments. Consequently, the asset dependent combatant commander may not have even a minimum assurance that the assets are available and will provide an acceptable level of mission success.

Commercial and industrial critical assets and infrastructures require a modified assessment process or processes that address their unique legal, contractual, and business needs, and the issues associated with threat development and sharing in the private sector and local government environment. Recent discussions with industry on vulnerability assessments identified a variety of concerns that will impact on the nature and scope of those assessments. Some of the concerns that CIP vulnerability assessment policies and procedures must resolve are the protection of proprietary information; the potential for impacting contractual obligations; contractual and other legal basis or agreements facilitating, allowing and authorizing an assessment; and maximizing the sharing of relevant threat information.

Existing vulnerability assessment efforts, chartered to satisfy other valid objectives, provide insight into aspects of CIP vulnerabilities; however, they tend to be installation oriented, highlighting possible installation vulnerabilities that may or may not have larger strategic implications. In most cases from a CIP perspective they are neither comprehensive nor integrated.

Lack of a coordinated assessment planning phase that identifies CIP goals and objectives to assessment organizations, as well as to specific organizations being assessed, is an obstacle to meeting CIP requirements through current assessment programs. This absence of coordinated planning further contributes to misunderstandings, differing expectations and inefficiencies regarding execution and reporting phases.

Lack of coordinated execution introduces the strong potential for confusion in the assessed organization. This confusion may include a perceived redundancy of assessments, uncertainty as to the intended end users for assessment products, and uncertain ownership of remediation and risk management decisions that will naturally flow from any assessment. Additionally, there are limited formal processes for tracking and follow up of assessment findings and little capability to identify and leverage resources to support remediation efforts.

Assessment information is not being re-used and each assessment team feels compelled to collect its own data, in part because of differences in focus among the different assessment disciplines. Even in the instances where different teams look at the same kinds of vulnerabilities, there are differences between assessment organizations as to assessment criteria, standards and protocols. We recognized that some assessment protocols rely primarily on professional judgment and experience and are therefore by their nature subjective to some extent. Subjective standards may limit the repeatability of results across assessments and therefore the confidence in scope and composition of the data among teams. It should be noted that subjective information collected or used by an assessment team does not per se preclude or inhibit information sharing. In some cases data collected by one team can be used by another; however differences in focus make this problematic on a wide-scale basis. As an example, JSIVA collects information on population centers and is interested in blast resistance of residential structures

(barracks, day-care centers, etc) because of their force protection mandate. A BSA going to a facility previously visited by a JSIVA would review JSIVA findings, but would not normally find information on population-independent vital mission areas (such as UPS buildings or Tech Control centers) because they are typically not a "Mass Casualty" concern.

Based on the results of the limited number of the OUSD(C3I) CIP Directorate-sponsored demonstration projects, the following lessons learned were provided:

- Designated assessment leader with the authority to provide direction and coordination
- Set reasonable goals and objectives
- Have a mission focus
- Manage expectations
- Stay flexible but resist requirements creep
- Clearly articulate roles and responsibilities for assessment providers, asset owners, and coordinating authority
- Use the chain of command for ownership of the asset
- Coordinate schedules well in advance
- Involve the Defense Infrastructure Sectors
- Ensure information sharing throughout the planning, execution and reporting phases
- Deliver an integrated report

## 2.3 QUESTION 3:

### **ARE THE PEOPLE WHO NEED THE ASSESSMENT RESULTS GETTING THE INFORMATION THEY NEED?**

**Finding 12:** No DoD coordinated process/policy/database currently exists for either identifying the existence of information or for providing access to the information itself to those responsible for risk management decisions.

**Finding 13:** No framework/process exists for identifying what information needs to be shared and for tailoring it to the needs of the users.

**Finding 14:** Aggregation of vulnerability data increases the requisite level of security classification.

**Discussion:**

Tasks 2, 4, 6, and 7 address the use of CIP vulnerability assessment information in planning, remediation, and mitigation efforts, how assessment information is shared and to whom it is provided, as well as the oversight, ownership, and management roles and responsibilities of the assessment organizations. The challenge we faced was to identify those CIP elements of information available from existing vulnerability assessments and to ensure this information be made available to the Services and resource owners so that they ensure CINC requirements are being met.

We found that each formal assessment mechanism currently has its own unique information distribution or sharing practices, some formal and “codified”, others informal and not designated in policy. The requesting headquarters of the organization or the commander of the organization being assessed typically receives a copy of the assessment report. CINC, Service and Agency Headquarters must establish coherent internal distribution policies that ensure that offices with infrastructure and asset responsibilities are fully informed of vulnerabilities. More significantly, information is not being shared for the following reasons: security concerns, the “being put on report” factor, and a lack of knowledge to whom information should be provided. There is no central repository of assessment and vulnerability information accessible to all need-to-know stakeholders. Further, there is no coordinated approach to mining the data from these assessments.

This finding is applicable to all levels from OSD, Joint Staff, CINCs, Services, and Agencies down to lower echelons. The point was made that some organizations with remediation or mitigation responsibilities are not getting vulnerability assessment information. There was a concern that risk management decisions made at the local unit command level might lack the “big picture” perspective.

Our consensus was that the information distribution process is flawed. We do not think it appropriate for us to make suggestions as to how the Services and Agencies fix an internal problem. We generally felt that an information sharing process would need to be brokered or refereed across Services and Agencies (with information provided to OSD, the Joint Staff, and assessment organizations) as in the case where an installation tenant comes from another Service. The JSIVA process was identified as a possible distribution model, in which the official requesting the assessment is asked to identify who should receive the information.

We agreed that the primary focus of information sharing should be to ensure that CINCs are provided with the (critical asset and infrastructure) information they need to understand the vulnerabilities of critical infrastructures and assets that support their operations/mission execution. In this manner they can conduct operational planning and ensure that the CINC needs are conveyed to asset owners who can address identified vulnerabilities. Concern centered on

the notion that the current assessment recipients may be accepting risks that the CINC is unaware of and that do not reflect CINC priorities.

There was general agreement that this information should be communicated to “responsible parties” who were characterized as having different objectives so would most probably have different levels of required information. The “responsible parties” were identified as:

- CINCs so that they understand the mission impact of asset/infrastructure degradation and make necessary risk management decisions, incorporate this information into OPLANs, and convey their priorities (e.g. through Integrated Priority Lists) to owners/operators.
- Services and Agencies as the asset and infrastructure owners and operators so they can make informed decisions about risk management, remediation and mitigation efforts, and modifying policy and procedures as necessary. The type of data to be received would depend on the needs of the Service or Agency.
- Assessment Community would use this data to improve assessment efficiency by changing practices and minimizing duplication, to conduct trend analyses, and to improve assessment effectiveness through an enhanced perspective from other views on the same problem.
- Sector leads and the CIP Directorate require this information for improved knowledge of the Defense Infrastructure Sectors and for setting policy, respectively.

The absence of a central repository does not imply the need for a single physical repository. A distributed, networked database with appropriate security measures could be a possible solution. We acknowledged that the required access to the data would entail significant problems that would need to be worked out in terms of policy, the sheer quantity of the data, and security concerns. As the repository grows, security and classification concerns for protecting the information will appropriately become more serious.

Finally, we expressed support for recommending that formal DoD policy and directives be established as to assessment practices, standards and information sharing. The Services and Agencies would be expected to develop their own processes consistent with these policies and directives.

## 3.0 RECOMMENDATIONS

### 3.1 VISION

We believe that a need exists for a coordinated, CIP vulnerability assessment process that supports CINC operational mission assurance. There is less of a need to establish an integrated, stand-alone assessment than there is to ensure coordination, shared protocols, information sharing and effective risk management based on existing assessments. To this end, we make the following recommendations. These recommendations are matched to tasks, with proposed implementation agencies, in Appendix E.

### 3.2 RECOMMENDATIONS

**Recommendation 1: Establish** clear and comprehensive DoD policy governing the CIP analysis and assessment processes.

This policy should address the following areas at a minimum:

- Analysis
  - Identification of critical assets
  - Prioritization (i.e., Tier 1-4)
  - Selection for assessment
- Assessment using existing programs
- Roles and responsibilities
  - Coordination and scheduling
  - Unique considerations for commercial and industrial assets
  - Information sharing
    - Report distribution
    - Relationship to existing assessments
    - Classification and aggregation issues
    - Protection of commercial proprietary information

**Implementation Recommendation 1a: Outline** in DoD policy the methodology for development and approval of tiered asset lists and for sharing these lists among the designated “need to know” components of the Department. This methodology should include compilation by the CINCs, Services and Agencies and review by the Critical Infrastructure Protection Integration Staff, vetting by the Joint Staff, and approval by OSD. DoD should complete the identification of Tier 1 and Tier 2 assets as quickly as possible.

**Implementation Recommendation 1b: Identify** clearly in DoD policy, the roles and responsibilities of OSD, the Joint Staff, CINCs, the Services, Agencies, Sectors, and assessment organizations in contributing to the CIP program. In the interim a technical

working group should be convened to draft a memorandum of agreement to be adopted by the above organizations and other DoD CIP stakeholders that establishes roles and responsibilities.

**Implementation Recommendation 1c: Establish** a technical working to study and recommend a process for coordinating existing vulnerability assessments and inspections. This technical working group should consider the JSIVA scheduling process as a possible model for the scheduling element of coordination.

**Implementation Recommendation 1d:** Specific to their needs, Services and Agencies should establish their own internal CIP vulnerability assessment report distribution processes.

**Recommendation 2: Develop** common vulnerability assessment protocols that support standardized outputs, relevant information sharing, and CIP risk-management decisions. This must follow the development of policy and procedures outlined in Recommendation 1.

**Implementation Recommendation 2a: Form** a technical working group with OSD and Joint Staff oversight to develop these protocols.

**Discussion:** In its work, the group should consider how to minimize the resources required to provide the necessary results. The protocols should allow for sufficient scalability to accommodate the expected variances in size, complexity, and other factors among the various assets and infrastructures to be assessed. One approach to developing a common protocol would be to develop common CIP-focused Essential Elements of Information (EEI) required and perhaps formats for these vulnerability assessment protocols. These EEIs can be used by assessment teams to provide compatibility in output between teams and great utility to CIP stakeholders.

**Implementation Recommendation 2b: Develop** as an additional product of this technical working group a CIP self-assessment tool for use by asset owners that can be used in conjunction with the threat assessment for the Commander's risk management responsibilities. This assessment tool should also be designed for use during pre-assessment visits to tailor the scope, nature and depth of the assessment. The self-assessment packages developed to support the NIVA and DISA/NSA should be examined as an example. Another example could be the self-assessment tools under development through DTRA's MIDAS program.

**Discussion:** In order to support the efforts of this technical working group it will be necessary to conduct a formal data call across the Department regarding on-going assessments that include infrastructure vulnerability as a designated element of examination. Data collection should include funding, preparation requirements, and statements of protocol. Alternatively, if the technical working group was composed of

knowledgeable assessment experts from all assessment organizations this might obviate the need for a data call.

**Implementation Recommendation 2c: Develop** the off-site commercial analysis of the JPO-STC as a standard preliminary tool for all infrastructure assessments. Develop a resource requirements baseline for this JPO-STC task based on all existing assessments that look at infrastructure.

**Implementation Recommendation 2d: Examine** the Balanced Survivability Assessment (BSA) conducted by DTRA as a model for a core assessment of mission critical infrastructure.

**Implementation Recommendation 2e: Continue** the OASD(C3I)/CIP assessment demonstration experiments as a platform to validate protocol development, i.e., scheduling, performance, reporting, information sharing, etc.

**Recommendation 3: Establish** a vulnerability assessment clearinghouse, with appropriate security safeguards, to support information sharing and assessment scheduling.

**Implementation Recommendation 3a: Develop** methods of cataloging and connecting all assessments, schedules, and reports, with a view towards implementing across the Department. This should include development of text search and link tools to allow rapid accessibility to infrastructure data across assessments and owners. Examine the USAF Inspector General's web-based system as an example.

**Implementation Recommendation 3b: Develop** a reporting method for vulnerability assessment information that will integrate and tailor information sharing as follows:

- By the CINC in understanding critical infrastructure impact on mission assurance
- Between assessment organizations for the purpose of conducting assessments
- By Services and Agencies conducting risk assessments and with Title 10 responsibilities in order to take corrective actions
- By Sectors supporting critical assets being assessed
- By installation hosts and tenants where corrective actions are to be made (this is especially important in cases where the tenant does not operationally report to the Service of the host installation)
- By OSD and the Joint Staff in providing risk assessments oversight

**Discussion:** An assessment conducted in support of the DoD CIP Program is a natural element of the Department's oversight role in ensuring continued ability to execute the National Military Strategy. The findings/vulnerabilities identified through the assessment process must be subject to operational risk management decisions by the Combatant Commanders. Where risks are found to be unacceptable, the Joint Planning and Execution Community, to include operational commands as well as asset owners, are



responsible to work together to take remediation, mitigation or other actions in support of the CINCs. In order to best support the entire process of reporting and risk management, the Joint Operational Planning and Execution System (JOPES) should serve as the methodology for integration of any assessment database. One example of a developing approach is the JPO's Infrastructure Systems Analysis and Assessment Capability.

**Implementation Recommendation 3c: Designate** an appropriate assessment agency or organization, such as the DoD Inspector General, a Service Inspector General, DTRA, or other agency, as the Executive Agent for vulnerability assessment throughout the DoD, with responsibility for coordinating scheduling, reviewing protocols, and maintaining data management tools.

## **APPENDIX A – CHARTER AND TERMS OF REFERENCE**

---

**FINAL**



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE  
6000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-6000

January 16, 2001

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Establishment of Integrated Vulnerability Assessment (IVA) Integrated Process Team (IPT)

This memorandum establishes the Integrated Vulnerability Assessment (IVA) Integrated Process Team (IPT). The Charter and Terms of Reference for the IPT are attached.

The purpose of the IPT is to develop the endstate and associated milestones to implement a Critical Infrastructure Protection integrated assessment process. The IPT must address current assessment initiatives with respect to funding, oversight control, scheduling, information requirements, and information sharing. The IPT must further investigate the applicability and feasibility of an integrated assessment process. In addition to current assessment initiative topics, the IPT must specifically address the intended assessment customer, products from the assessment, distribution of assessment products, frequency of assessments, individual assessments that should/could be integrated, and the agency/service that would own/fund and provide oversight of any new integrated assessment process.

The IPT will be co-chaired by representatives from the OASD (C3I) CIP Directorate and the Joint Staff (J-5), and it will be comprised of representatives from OSD, the Joint Staff (J-2, J-34, J-39, J-6, J-4 and J-7), ASD (SO/LIC), the Services, USTRANSCOM, JPO-STC, DTRA, DISA, DLA, DSS and NSA.

We have scheduled the IPT kick-off meeting for January 18, 2001 at 1300 in Crystal Gateway 1, Room 802. Request you submit the names of your primary and alternate representatives to serve on this IPT to my point of contact, Ms. Jo MacMichael, jo.macmichael@osd.mil, phone (703) 602-5874, by January 17, 2001.

J. William Leonard  
Deputy Assistant Secretary of Defense  
(Security and Information Operations)

Attachments



FINAL

**DISTRIBUTION:**

ASSISTANT SECRETARY OF DEFENSE, SPECIAL  
OPERATIONS, LOW INTENSITY CONFLICT (CTP&S)  
DEPARTMENT OF THE AIR FORCE (AF/SCM)  
DEPARTMENT OF THE ARMY (DAMO-OD)  
DEPARTMENT OF THE NAVY (DON CIO)  
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (NS5)  
DIRECTOR, DEFENSE LOGISTICS AGENCY (J34)  
DIRECTOR, DEFENSE SECURITY SERVICE (DS2)  
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY (DTRA/CS/TD)  
DIRECTOR, NATIONAL SECURITY AGENCY (NSA/X GROUP)  
DIRECTOR, JOINT STAFF  
JOINT PROGRAM OFFICE FOR SPECIAL TECHNOLOGY  
COUNTERMEASURES  
USTRANSCOM (TCJ5V)

---

**FINAL**

---

**CHARTER FOR OSD/JOINT STAFF INTEGRATED VULNERABILITY ASSESSMENT  
(IVA) PROCESS INTEGRATED PROCESS TEAM (IPT)**

**OBJECTIVES:**

1. Study the viability of an Integrated Vulnerability Assessment (IVA) with respect to Critical Infrastructure Protection (CIP). The study should maximize to the largest extent possible existing assessments and assessment protocols.
2. Study methods of linking the assessment process with required CINC OPLAN/Appendix reviews to maximize the application of assessment lessons learned.
3. Make recommendations to the IVA Steering Committee on the implementation of an IVA process.

**RESPONSIBILITIES:**

1. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/CIP Directorate and the Joint Staff (J-5) will sponsor the IVA IPT and provide joint direction and guidance and serve as the Steering Committee.
2. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/CIP Directorate and the Joint Staff (J-5) will appoint representatives to co-chair the IPT.
3. The IVA IPT membership will consist of representatives from the OSD, Joint Staff (J-2, J-34, J-39, J-6K, J-4 and J-7), ASD (SO/LIC), the Services, JPO-STC, USTRANSCOM, DTRA, DISA, DLA, DSS, and NSA. Appropriate subject matter experts will be invited to participate as determined necessary by the IPT.

**TASKS:**

1. Study the current assessment processes to determine the authority/policy source for individual assessment mandates, the applicable standards and documentary authority for the associated assessment standards, how individual assessments are scheduled, the required frequency of assessments, specific data collection requirements, and the required reports/distribution of reports.
2. Study the CIP specific assessment requirements. Answer the questions – “What do we want to assess?”, “Why do we need/want to assess?”, “What will we do with the information when we have gathered it?”, “Who needs to know?”, “What form do the results need to be promulgated in?” “What additional security requirements have we created in an IVA process?”

3. Explore methods to synergize current individual assessments that might directly support CIP. Assessment integration would focus on reduction of any redundancies, development of clear assessment standards, development of common protocols for assessment, streamline scheduling, and economize funding. Any effort to combine assessments must be consistent with existing policy directives or recommend appropriate changes to policy directives for assessments.
4. Make recommendations on how the results of CIP assessments should be used in planning, mitigation, and remediation. Determine how to best use the collected data to ensure that appropriate CIP remediation/mitigation measures are implemented.
5. Develop a process, with timelines, for the planning, coordination, and scheduling of IVA assessments. Address timelines for generation, coordination and review of IVA reports.
6. Determine how, to whom, and in what format the IVA results should be distributed.
7. Conduct a review of organizational roles and responsibilities to determine the most appropriate organizational location for the oversight, ownership, and management of an IVA Teams and process.

**REPORTS:**

Final report due 4 months after start date. Provide monthly In Process Reviews to the IVA Steering Committee.

---

**OSD/JOINT STAFF INTEGRATED VULNERABILITY ASSESSMENT (IVA) PROCESS  
INTEGRATED PROCESS TEAM (IPT)**

**TERMS OF REFERENCE (TOR)**

The IPT process is designed to facilitate decision-making by taking advantage of the team members' expertise and by making decisions and recommendations based on timely input from the key stakeholders and replaces a lengthy sequential review and approval process.

The IPT shall function in a spirit of teamwork with participants empowered and authorized, to the maximum extent possible, to make commitments for the organization or the functional area they represent. Empowerment is critical to making and keeping the agreements essential to an effective IPT. All representatives assigned to the IPT must be empowered by their leadership. They must be able to speak for their superiors, in the decision-making process. IPT members cannot be expected to have the breadth of knowledge and experience of their leadership in all cases. However, they are expected to be in frequent communication with their leadership, and thus ensure that their advice is sound and will not be changed later, barring unforeseen circumstances or new information.

The IPT charter will be drafted by the co-chairs, ratified by the membership at the outset of the IPT, and approved by the Steering Committee.

The co-chairs should clearly articulate the IPT's focus at the outset of the process and should ensure that the goals and objectives of team members are consistent with the project goals and objectives. An effective mechanism to provide performance feedback to team members and their functional organization should be established.

Each team member brings to the team unique experience that needs to be recognized by all. Because of that expertise, each person's views are important in developing a successful program, and these views need to be heard. Teams must have full and open discussions with no secrets. Full and open discussion does not mean that the team must act on each view, but all facts must be on the table for each team member to understand and assess. Cooperation is essential. The team is not searching for "lowest common denominator" consensus. There can be disagreement on how to approach a particular issue, but disagreement must be reasoned disagreement based on an alternative plan of action rather than unyielding opposition. Team members should openly raise and discuss issues at the earliest possible opportunity. The IPT should try to resolve issues within the team, seeking additional functional expertise when necessary. In the spirit of teaming and cooperation, issues should not be worked "off-line" beyond the purview of the IPT. Issues that cannot be resolved by the team must be identified early so that resolution can be achieved as quickly as possible at the appropriate level.

A sense of ownership on the part of the IPT members is key to the success of the IPT process. Ownership is a collective concept. All IPT members must feel that their contributions are important to the process and are well considered. Decisions and documents should be a product of the team.

Once established, the IPT should meet as often as necessary to meet its objectives. With that focus, the IPT should only meet for a particular purpose at a scheduled time. It should not meet regularly or continuously in an "update" mode. To ensure productive meetings, detailed agendas with timelines for topics and supporting material must be distributed at least three business days before the meeting rather than at the meeting. Every effort should be made to use electronic media for distribution. Meeting minutes should be provided to the IPT members within one working day of a meeting. Meeting minutes should be accurate and brief, but detailed enough to preclude revisiting previous agreements and wasting the time and resources of the team members. Meeting minutes should record attendance, document any decisions or agreements reached by the IPT, document action items and suspense, set the agenda for the next meeting, and capture those issues framed for higher-level resolution.



## **APPENDIX B – LIST OF REPRESENTATIVES**

---

**FINAL**

## PRIMARY AND ALTERNATE REPRESENTATIVES

<b>Co-Chairs</b>	
Joint Staff (J-5)	
	LtCol Mark Murphy - co-chair of the IPT. CIP Action Officer in J-5 Global Division, Joint Staff. Participated in the Joint Staff's CIP Mission Analysis, DoD Directive Review, and drafting of CJCS Instruction and JOPES Planning Guidance. Joint Staff representative to CIPIS.
OASD(C3I)	
	Mrs. Jo MacMichael - co-chair of the IPT. Financial Manager in CIP Directorate, OASD(C3I). Participated in OMB CIP/IA data call and FY01 Program / Budget Reviews. Focal point for CIAO Council meetings.
<b>Participants</b>	
Air Force	
	Mrs. Deborah Gallo – Department of the Air Force primary representative to IPT - USAF CIP Action Officer (ANSER) - Information Assurance Division, Deputy Chief of Staff, United States Air Force.
	Maj. Mel Allen – Department of Air Force alternate representative to IPT - HQ USAF/XOFP, Security Forces Directorate, Force Protection and Operations Division, Antiterrorism Action Officer. Provided information and input about the AF vulnerability assessment program.
	Maj Joe Castro - Department of Air Force alternate representative to IPT - AF Installations and Logistics Representative for CIP, Readiness Program Manager, Readiness & Installation Support Division, Office of The Civil Engineer, Headquarters Air Force.
Army	
	Mr. John S. Tomko, Jr. – Department of the Army representative to IPT -Program Analyst: Army Infrastructure Assurance; Military Support Division, Operations, Readiness and Mobilization Directorate, Headquarters Department of the Army
	LTC Donna Rivera – Army briefer - Chief, Physical Security Branch, HQDA. Responsible for developing policies and procedures for physical security measures, and identifying equipment requirements for the security of all Army assets, including nuclear, chemical and arms, ammunition and explosives. Responsibilities also include the management, training and certification standards of the security forces, including the military working dog teams.
ASD (SO/LIC)	
	Mr. Donald Lapham - ASD (SO/LIC) representative to the IPT - Assistant for Antiterrorism Policy in Combating Terrorism Policy and Support Directorate, OASD (SO/LIC). Responsible for development and oversight of antiterrorism policy for all DoD activities.
Booz·Allen & Hamilton	

FINAL

	Mr. Kevin Moody - Booz Allen & Hamilton contractor supporting the OASD (C3I) CIP Directorate. Supports the IPT, CIPIS, and provides management and technical support.
DISA	
	Mr. Dave Hughes - DISA representative to IPT. Chief of DISA's Field Security Operations Branch (FSO). Responsible for Technical INFOSEC Assessments of DISA Field Operating Facilities and INFOSEC Support to the CINCs. FSO has extensive published guidance on how to secure computer operating systems & networks and how to review them.
DLA	
	Mr. Timothy Barb – DLA representative to IPT - Chief, Intelligence/Security Division, Command Security, DLA Support Services.
	Mr. Larry Johnson – DLA alternate representative to IPT – Information Assurance Division (J-633), Information Operations Directorate, Defense Logistic Agency
DOT	
	CDR . Dan McClellan, USCG/MARAD/DOT representative to IPT - Deputy Associate Director for National Security Policy, Office of Intelligence and Security (OIS). OIS is the program office for PDD-63/CIP activities within DOT.
DSS	
	Mr. Mike Berry – DSS representative to IPT. Chief, Policy, Industrial Security Program Office (ISPO). ISPO primarily oversees US cleared contractors in their protection of classified information. Responsible for development of DSS CIP support. Active participant at the National and OSD levels in developing asset and infrastructure protection policies and guidance and interagency cooperation from 1998 to present.
	Mr. Richard Lawhorn – DSS alternate representative to IPT. Chief, Operations, ISPO.
DTRA/CSA	
	Col. Len Blevins – DTRA/CSA primary representative to IPT – As the Chief of the Combat Support Antiterrorism Division, manages the Joint Staff Integrated Vulnerability program and represents DTRA to federal, state, local and foreign government agencies and related organizations on AT/FP matters.
	Mr. Michael Guarracino – DTRA/CSA alternate representative to IPT - Deputy Division Chief, Combat Support, Anti-Terrorism Assessments Division, Defense Threat Reduction Agency (DTRA).
DTRA/CSOB	
	Mr. Dave Lewis - DTRA/CSOB primary representative to IPT - Technical Chief, Combat Support, Balanced Survivability Assessments Division. Responsible for Blue / Red BSA Assessments Programs and serves as Team Chief on DTRA's special BSA teams.
	Matt Leavitt – DTRA alternate representative to IPT - DTRA Contractor. Serves as Senior Engineer on DTRA's BSA Teams; primary focus on Damage Control / Emergency Response and Reconstitution. Assigned duties as BSA training manager.
	Mr. Steve Chin - Alternate DTRA government representative to IPT - primary CIPIS POC. Primary scheduling coordinator for BSA Blue Teams, and serves as Team Chief on BSA Blue Team assessments.

**FINAL**

Joint Staff (J-2)	
	Mr. Toby Philbin – J-2 representative to IPT – career intelligence officer from DIA. Temporarily detailed to work with both CIP and Defense Information Assurance Program in support of interlocking information superiority objectives and as an advisor to the Defense Science Board.
Joint Staff (J-34)	
	LTC John Quackenbush – J-34 representative to IPT - Senior Assessments Officer in J-34, Combatting Terrorism, Joint Staff. CIP Action officer in J-34. Participated in the Joint Staff's CIP Mission Analysis, DoD Directive Review, and drafting of CJCS Instruction and JOPES Planning Guidance.
Joint Staff (J-39)	
	LTC William Dallas - J39 representative to IPT - Computer Network Defense (CND) Officer for Joint Staff. CIP/CND Officer in J-39. Participated in the Joint Staff's CIP Mission Analysis, DoD Directive Review, and drafting of CJCS Instruction and JOPES Planning Guidance.
	CDR Paul Thrasher - J39 representative to IPT - Computer Network Defense (CND) Officer for Joint Staff. CIP/CND Officer in J-39. Participated in the Joint Staff's CIP Mission Analysis, DoD Directive Review, and drafting of CJCS Instruction and JOPES Planning Guidance.
Joint Staff (J-4)	
	CDR Jerry Reid – J-4 representative to IPT. CIP Action Officer in Joint Staff, J-4, Deployment Division. Participated in the Joint Staff CIP Mission Analysis, DoD Directive Review, and drafting of CJCS Instruction and JOPES Planning Guidance.
	CDR Eric Odderstol CEC, USN – J-4 engineering representative to IPT. Action Officer assigned to JCS J4 Engineer Division. Responsible for Class II property/facilities. Ensure CINCs consider CIP as they develop Civil Engineering Plan (CESP).
Joint Staff (J-6)	
	LTC Vic Butera - J-6 representative to IPT. Lead Action Officer for cyber protection/Information Assurance aspects of CIP in Joint Staff J-6 Information Assurance Division.
Joint Staff (J-7)	
	Col Gary Snyder - J7 representative to IPT. CIP Action Officer in J7 Directorate, the Joint Staff. Participated in DoD Directive Review and drafting of CJCS Instruction and JOPES Planning Guidance. Regional Plans Branch Chief and EUCOM NATO regional officer.
JPO/STC	
	John Keenan – JPO-STC representative to IPT. Deputy Program Manager for the Joint Program Office for Special Technology Countermeasures' Infrastructure Assurance Program. Participated in the development and establishment of the CIP concept from pre-CAAP and pre-PDD-63 days. Directly supports OASD(C3I) as their Technical Direction Agent for CIP matters.
Mitretek	
	Mr. Dan Schultz - Mitretek support to OASD (C3I) CIP Directorate. Prepared draft IVA IPT MFRs, presented Malmstrom AFB briefing, collaborated on preparation of IVA IPT

**FINAL**

	Final Report. Participated in DIVA concept development.
Navy	
	Mr. Hank Chase - DON representative to IPT. DON CIP Assessment Lead. Vredenburg & Company supporting DON CIAO and representing Asst. SECNAV for Installations and Environment (I&E). Retired Navy CEC Commander. Responsible for all facilities and utilities CIP issues affecting DON Installations.
	Mr. Bill Bramer - Navy attendee and briefer. Physical Security Specialist. Assigned to both N34 (Antiterrorism/Force Protection Division) and NCIS Code 24 (Law Enforcement/Physical Security Directorate of NCIS). In N34: Assistant to Plans and Assessments Branch Head for protocols and scheduling of Antiterrorism/Force Protection Integrated Vulnerability Assessments Navy-wide. Representative to Service Working Groups for development of software products (such as Joint Vulnerability Assessment Tool). Representative to DoN CIAO Working Group for OPNAV N34. In NCIS: Assistant to Plans and Assessments Division Head, responsible for all physical security policy in Navy and Marine Corps. Dual-hatted shop that works both at the CNO level and the ASN level as required.
	Mr. James Cain – Marine Corps attendee and briefer. Head, Antiterrorism/Physical Security Section, Headquarters Marine Corps, Law Enforcement and Security Branch (POS). Assistant to the Director, Operations Division. Responsible for Marine Corps Antiterrorism and Physical Security Programs; Program Manager for Marine Corps Electronic Security Systems Program. Responsible for Marine Corps Integrated Vulnerability Assessments and coordination of JSIVAs for The Marine Corps. Representative to the PSEAG, TSWG, etc. POS responsible to the Director of Operations, and the Assistant Commandant for Plans, Policies, and Operations.
NIMA	
	Ms. Nicole Felini- ISR Sector observer. Booz Allen & Hamilton contractor supporting the National Imagery and Mapping Agency Continuity Planning Division. Regular participant in the ISR Sector and CIPIS.
	Mr. John Donnelly – ISR Sector observer. Deputy Chief, Continuity Planning Division and Deputy CIAO, National Imagery and Mapping Agency. Regular participant in the ISR Sector, CIPIS and Intelligence Community's Continuity of Operations fora.
National Security Agency (NSA)	
	Mr. Gregory W. Hale, Sr. - NSA representative to IPT - Senior Operations Staff Officer for NSA X6, the Operations Readiness and Assessments Office. Supporting the OASD/C3I DIAP Information Assurance Readiness Metrics Working Group, the IAP DITSCAP Working Group, and was the interim NSA representative on the OASD/C3I Certification and Accreditation of Computer Network Defense Service Providers Working Group.
	Mr. Wilbur J. Hildebrand Jr. – NSA alternate representative to IPT - Chief, INFOSEC Vulnerability Assessment Services Division (X61), National Security Agency. Previously NSA's representative and lead member of the Critical Infrastructure Assurance Office (CIAO) Phase I and Phase II Critical Infrastructure Protection Plan Expert Review Team.
	Ms. Rebecca Canfield – NSA alternate representative to IPT - Deputy Chief, INFOSEC

---

**FINAL**

	Vulnerability Assessment Services Division (X61), National Security Agency.
	Ms. Tamara S. Cook - NSA alternate representative to IPT - Representative of the Interagency OPSEC Support Staff (X63), National Security Agency .
OASD(C3I)	
	Mr. Frank Dixon – observer. Lead for the Rocky Mountain Corridor Critical Infrastructure Protection Analysis and Assessment effort in the OASD (C3I) CIP Directorate. On detail from the Joint Program Office for Special Technology Countermeasures.
	Major John J. Kaplan – observer. Program Manager for DTRA’s Mission Degradation Analysis (MIDAS) program. Managing the MIDAS R&D effort to develop toolset framework for assessments including self-assessment modules and modeler modules. Managing the MIDAS R&D effort to assess future infrastructures prior to their installation to design appropriate protection into the infrastructures.
SAIC	
	Dr. Robert J. Coullahan, CEM – Invited participant and briefer. Assistant Vice President and Manager, Readiness & Response Division, Science Applications International Corporation (SAIC); Requirements Task Lead for the DTRA Mission Degradation Analysis (MIDAS) Program.
USTRANSCOM	
	Mr. Al Colvin – USTRANSCOM representative to IPT. Participated in the drafting of the DoD CIP Directive, Security Classification Guide, CJCS Instruction, and JOPES Planning Guidance. USTRANSCOM CIP Program Manager for Transportation Sector, and representative to CIP Integration Staff.

## **APPENDIX C – RELATIONSHIP OF TASKS TO QUESTIONS**

---

**FINAL**

C-1

QUESTIONS	TASKS
<p>Question 1:</p> <p>Are we satisfying CIP requirements for determining if critical assets are vulnerable?</p>	<p><u>Task 1:</u></p> <p>Study the current assessment process to determine:</p> <ul style="list-style-type: none"> <li>• Authority/policy mandates</li> <li>• Standards and their authority</li> <li>• Scheduling and frequency</li> <li>• Specific data collection requirements</li> <li>• Required reports and distribution</li> </ul> <p><u>Task 2:</u></p> <p>Study the CIP specific assessment requirements</p> <ul style="list-style-type: none"> <li>• What do we want to assess?</li> <li>• Why do we need/want to assess?</li> </ul>
<p>Question 2:</p> <p>Are we <u>collecting</u> information effectively (scheduling) and efficiently (timing)?</p>	<p><u>Task 3:</u></p> <p>Explore methods to synergize current individual assessments that might directly support CIP</p> <ul style="list-style-type: none"> <li>• Reduction of any redundancies</li> <li>• Development of assessment standards</li> <li>• Development of common assessment protocols</li> </ul> <p><u>Task 5:</u></p> <p>Develop a process, with timelines for planning, coordination, and scheduling of IVA assessments</p> <ul style="list-style-type: none"> <li>• Address timelines for generation, coordination, and review of IVA reports</li> </ul> <p><u>Task 7:</u></p> <p>Conduct a review of organizational roles and responsibilities to determine the most appropriate location for</p> <ul style="list-style-type: none"> <li>• Oversight</li> <li>• Ownership</li> <li>• Management</li> </ul> <p>of the IVA Teams and process</p>



QUESTIONS	TASKS
<p>Question 3: Information sharing. Are the people who need information getting it?</p> <p>Question 3: (continued) Information sharing. Are the people who need information getting it?</p>	<p><u>Task 2:</u> Study the CIP specific assessment requirements</p> <ul style="list-style-type: none"> <li>• What will we do with the information?</li> <li>• Who needs to know?</li> <li>• What form for promulgation?</li> <li>• What additional security requirements have we created in an IVA process?</li> </ul> <p><u>Task 4:</u> Make recommendations on how results of CIP assessments should be used in Planning, Mitigation and Remediation</p> <ul style="list-style-type: none"> <li>• Determine how to best use the collected data to ensure that appropriate CIP remediation/mitigation measures are implemented</li> </ul> <p><u>Task 6:</u> Determine how, to whom, and in what format the IVA results should be distributed</p> <p><u>Task 7:</u> Conduct a review of organizational roles and responsibilities to determine the most appropriate location for</p> <ul style="list-style-type: none"> <li>• Oversight</li> <li>• Ownership</li> <li>• Management</li> </ul> <p>of the IVA Teams and process</p>

## **APPENDIX D – ASSESSMENT MATRIX**

**(See File “Appx D\_IVA IPT Matrix.xls”)**

## **APPENDIX E – RECOMMENDATIONS MATRIX**

---

**FINAL**

<b>RECOMMENDATION</b>	<b>FINDING</b>	<b>OPR</b>	<b>IMPLEMENTER</b>	<b>IMPLEMENTATION DATE</b>	<b>FINAL PRODUCT</b>	<b>COMPLETION DATE</b>
1. Policy	4, 8	OSD CIP	DoD Instruction	Draft Jul 01	Signed instruction	Jan 02
1a. Tiered asset list	4, 6	OSD CIP	DoD Instruction	Draft Jul 01	Signed instruction	Jan 02
1b. Roles & responsibilities	4, 7, 8	OSD CIP	DoD Instruction	Draft Jul 01	Signed instruction	Jan 02
1c. Coordination & scheduling	7, 8	ASD C3I	Initiate Working Group	Aug 01	FY 02 Schedule	Oct 01
1d. Internal report distribution	9, 10, 12, 13, 14	Service Agency	-----	-----	-----	-----
2. Common protocols	1, 2, 5	Tech Work Group	Study and Drafting Sessions	Nov 01	Consolidated Protocol	Aug 02
2a. Form tech working group	1, 2	ASD C3I	ASD Memo	Sep 01	Consolidated Protocol	Aug 02
2b. Self-assessment tool	1, 2, 4	Tech Work Group	ASD Memo	Sep 01	Approved Self-assessment	Aug 02
2c. Develop JPO-STC product and resource base	2	Tech Work Group	ASD Memo	Sep 01	Resource Request	Feb 02
2d. Examine BSA as basic CIP assessment	2	Tech Work Group	ASD Memo	Sep 01	BSA Review	Feb 02
2e. Demonstration projects	2, 5, 7, 9, 13	OSD CIP	ASD Memo	On going	CIP Assessment Work Plan	Feb 02

**FINAL**

<b>RECOMMENDATION</b>	<b>FINDING</b>	<b>OPR</b>	<b>IMPLEMENTER</b>	<b>IMPLEMENTATION DATE</b>	<b>FINAL PRODUCT</b>	<b>COMPLETION DATE</b>
3. Assessment clearinghouse	8, 9, 10, 11, 12, 13, 14	ASD C3I	ASD Memo	Sep 01	Web-linked database	Jan 02
3a. Report sharing & distribution system	9, 10, 12, 13, 14	Tech Work Group	ASD Memo	Sep 01	Work Group Draft	Jan 02
3b. Develop common reporting method	10, 12, 13, 14	Tech Work Group	ASD Memo	Sep 01	Standard Report Format	Aug 02
3c. Designate Executive Agent	8	ASD C3I	ASD Working Group	Oct 01	DepSecDef Memo	Oct 02

---

**FINAL**

## **APPENDIX F – BRIEFINGS**

---

**FINAL**

**APPENDIX F1 – DOD INTEGRATED VULNERABILITY ASSESSMENT (DIVA)**

---

**FINAL**

## **APPENDIX F2 – ROCKY MOUNTAIN EFFORT**

---

**FINAL**

F2-1



**APPENDIX F3 – CRITICAL INFRASTRUCTURE PROTECTION (CIP) ANALYSIS &  
ASSESSMENT CRITICALITY**

---

**FINAL**

## **APPENDIX F4 – MISSION DEGRADATION ANALYSIS PROJECT OVERVIEW**

---

**FINAL**

**APPENDIX F5 – NATIONAL SECURITY AGENCY INFORMATION ASSURANCE  
ASSESSMENTS**

---

**FINAL**

## **APPENDIX F6 – AT/FP PROGRAM OVERVIEW**

---

**FINAL**

## **APPENDIX F7 – BALANCED SURVIVABILITY ASSESSMENTS**

---

**FINAL**

F7-1

**APPENDIX F8 – DEFENSE SECURITY SERVICE INDUSTRIAL SECURITY  
PROGRAM (FACILITY SECURITY CLEARANCE AND SECURITY REVIEW  
PROCESSES)**

---

**FINAL**

## **APPENDIX F9 – DISA'S SECURITY READINESS REVIEW (SRR) PROCESS**

---

**FINAL**

**APPENDIX F10 – JPO-STC INFRASTRUCTURE ASSURANCE PROGRAM  
OVERVIEW FOR THE IVA-IPT**

---

**FINAL**

F10-1



## **APPENDIX F11 – AIR FORCE VULNERABILITY ASSESSMENTS**

---

**FINAL**

F11-1

**APPENDIX F12 – INFORMATION BRIEFING FOR: INTEGRATED  
VULNERABILITY ASSESMENT INTEGRATED PROCESS TEAM (USTRANSCOM)**

---

**FINAL**

F12-1

**APPENDIX F13 – SECURITY, FORCE PROTECTION, AND LAW ENFORCEMENT  
DIVISION, ODCSOPS**

---

**FINAL**

F13-1

## **APPENDIX F14 – THE DLA COMBATING TERRORISM PROGRAM**

---

**FINAL**

F14-1

**APPENDIX F15 – NAVAL INTEGRATED VULNERABILITY ASSESSMENT (NIVA)**

---

**FINAL**

F15-1

**APPENDIX F16 – CHIEF OF NAVAL OPERATIONS INTEGRATED  
VULNERABILITY ASSESSMENT (CNOIVA) PROGRAM**

---

**FINAL**

F16-1

**APPENDIX F17 – ARMY INFRASTRUCTURE ASSURANCE XXI**

---

**FINAL**

F17-1

**APPENDIX F18 – MARINE CORPS INTEGRATED VULNERABILITY ASSESSMENT  
(MCIVA)**

---

**FINAL**

F18-1



**APPENDIX F19 – COMBATANT COMMAND SUPPORT DESIRES CIP  
VULNERABILITY ASSESSMENT**

---

**FINAL**

F19-1

**APPENDIX F20 – IVA NOTIONAL TIMELINE MATRIX (SPREADSHEET)**

---

**FINAL**

F20-1

**APPENDIX F21 – PACNORWEST CIP ANALYSIS AND ASSESSMENT PROCESS  
LESSONS LEARNED**

---

**FINAL**

F21-1

## **APPENDIX F22 – MALMSTROM AFB ASSESSMENT**

---

**FINAL**

F22-1

## **APPENDIX F23 – ROCKY MOUNTAIN EFFORT (RMC) LESSONS LEARNED**

---

**FINAL**

F23-1

**APPENDIX F24 – JSIVA SCHEDULING PROCESS (JOINT STAFF INTEGRATED  
VULNERABILITY ASSESSMENT)**

---

**FINAL**

F24-1